Effective date: 1 February 2007, amended 17 December 2010

SEC-100 Accountability Framework for CSEC Security

1. Overview

1.1 Purpose

This document is the accountability framework for the corporate security function within CSEC. It outlines roles and responsibilities primarily at the senior management level.

1.2 Authority

Treasury Board of Canada Secretariat (TBS) *Policy on Government Security (PGS)* (July 2009):

"Deputy heads of all departments are responsible for establishing a security program for the coordination and management of departmental security activities that has a governance structure with clear accountabilities." (section 6.1.1, Requirements)

1.3 Approval

The CSEC Security Committee approved this amendment on 17 December 2010.

1.4 Context

The *PGS* and its attendant directives and operational security standards list most security roles and responsibilities that federal departments must assign. In addition to these, the SEC-100 framework includes accountabilities that stem from technical security standards produced by lead agencies under the *PGS*.

CSEC is the lead agency for producing standards for the security of SIGINT and COMSEC. Accordingly, CSEC must assign responsibility centres to fulfill those roles as outlined in the technical security standards. These additional authority references, including some internal CSEC security policies, are cited in section 3.1 below.

Continued on next page

1. Overview, continued

1.5 Accountability Centres

The following table lists CSEC's primary accountability centres for security functions.

1.5.1 Accountability Centres for Security Functions	1. Chief, CSEC 2. Deputy Chief, Corporate Services, through • Director General, Corporate Services Operations • Director General, Finance • Director General, Human Resources 3. Deputy Chief, SIGINT, through • Director General, Programs 4. SIGINT Directors General 5. Deputy Chief, IT Security 6. Chief Information Officer 7. Director General, Audit, Evaluation and Ethics 8. Director General, Policy & Communications 9. Director, Corporate Security 10. Director, Information Security 11. Managers 12. Group Security Officers 13. Personnel 14. Security Committee

2. CSEC Security Accountabilities

2.1 Chief, CSEC (CCSEC)

The Chief's roles and responsibilities for security stem from the following sources:

- The Ministerial Directive, *CSE Accountability Framework* (June 19, 2001), requires accountability to the Deputy Minister of National Defence (DMND) for administrative matters including security; some specific points are:
    - Maintaining appropriate safeguards when entering into arrangements with other organizations;
    - Balancing the requirement for adequate security measures with sensitivity to the impact that it might have on the professional and private lives of CSEC's employees; and,
    - Reporting annually on CSEC's performance and management issues of significance.
- Under the *Canadian SIGINT Security Standards (CSSS),* the Chief is CSEC's Senior Indoctrinated Official (SIO).
- The Chief may recommend to the DMND the revocation or denial of a security clearance, and the designation of individuals permanently bound to secrecy under the *Security of Information Act*.

2.2 Deputy Chief, Corporate Services (DCCS)

The Deputy Chief, Corporate Services (DCCS), is accountable to the CCSEC for the following portfolios: finance, human resources, and corporate services operations (which includes corporate security).

2.2.1 Director General, Corporate Services Operations (DG CS Ops)

As the Departmental Security Officer (DSO), the Director General, Corporate Services Operations (DG CS Ops), is accountable to the DCCS for the corporate security and emergency management programs*, and for coordinating with other accountability centres below in discharging various aspects of these programs.

* delegated to the Directors for Corporate Security and Program Management.

Continued on next page

2. CSEC Security Accountabilities, continued

2.2.2 Director General, Finance (DGF)

The Director General, Finance (DGF), is CSEC's contracting authority and is accountable to the DCCS for*:

- Ensuring that security requirements are included in procurement transactions.

* delegated to the Manager, Contracting and Procurement.

2.2.3 Director General, Human Resources (DGHR)

The Director General, Human Resources (DGHR), is accountable to the DCCS for:

- Consulting with, and recommending to management, appropriate remedial action (including disciplinary sanctions) for security incidents; and,
- Administering CSEC's Occupational Health and Safety (OHS) program.

2.2.4 Director General, Policy and Communications (DGPC)

The Director General, Policy and Communications (DGPC), is accountable to the CCSEC for*:

- Developing and promulgating operational policies and procedures for SIGINT and ITS;
- Providing advice and guidance on operational policy;
- Supporting DGP in the coordination of damage assessments regarding SIGINT-related incidents; and,
- Supporting the DCS in security incident investigations.

* delegated to the Director, Operational and Corporate Policy.

2.3 Deputy Chief, SIGINT (DCSIGINT)

The Deputy Chief, SIGINT (DCSIGINT), is accountable to the CCSEC for most aspects of SIGINT security, including these roles:

- Departmental Communications Intelligence (COMINT) Control Officer (COMCO), as per the *CSSS*;
- Exceptionally Controlled Information (ECI) System Owner*;
- SIGINT Operational Authority for all CSEC internal IT systems used to convey/handle SIGINT information*; and,

* delegated to the Director General, Programs (DGP).

Continued on next page

2. CSEC Security Accountabilities, continued

2.3 Deputy Chief, SIGINT (DCSIGINT), continued

- Indoctrinating senior officials for SIGINT Information Access*.

  Note: "senior officials" include:
  - the CSE Commissioner;
  - the National Security Advisor to the Prime Minister;
  - Ministers;
  - Deputy Ministers; and,
  - Ministerial Executive Staff.

* delegated to the Director General, Programs (DGP).

2.3.1 Director General, Programs (DGP)

The Director General, (SIGINT) Programs (DGP), is accountable to the DCSIGINT for*:

- Granting the "Authority to Operate" for all CSEC internal IT systems used to convey or handle SIGINT information;
- Administering the ECI program;
- Administering the GAMMA sub-control system;
- Coordinating damage assessments regarding SIGINT-related incidents;
- Being the departmental coordinator or point of contact for SIGINT security advice, guidance and education to GC entities;
- Establishing and maintaining the policy framework and procedures for the control and distribution of SIGINT; and,
- Supporting the Director, Corporate Security (DCS), in security incident investigations and conducting follow-up.

* delegated to the Director, (SIGINT) Requirements.

2.3.2 SIGINT Directors General (DGs) / ECI Managers

SIGINT Directors General (DGs), in whose directorate ECI compartments are managed, are responsible for indoctrinating senior officials from other GC departments into those ECI compartments.

Continued on next page

2. CSEC Security Accountabilities, continued

2.4 Deputy Chief, IT Security (DCITS)

The Deputy Chief, IT Security (DCITS), is accountable to the CCSEC for:

- Exchanging IT security incident-related information with other GC departments; and,
- Appointing a COMSEC Custodian*, as per the TBS Operational Standard on the *Management of IT Security* (*MITS)*.

* delegated to the Director, Crypto Material Systems and Services.

2.5 Chief Information Officer (CIO)

The Chief Information Officer (CIO) is accountable to the CCSEC for:

- CSEC's IT security program and risk mitigation, including the certification and accreditation of CSEC IT systems, and of Government of Canada (GC) systems connected to CSEC's classified network;
- IM/IT security management issues and providing advice and guidance on IT security policy;
- Coordinating the IM/IT security function with the DCS; and,
- Managing the IT Security Coordinator (ITSC) function.

2.6 Director General, Audit, Evaluation & Ethics (DGAEE)

The Director General, Audit, Evaluation and Ethics (DGAEE), is accountable to the CCSEC for:

- Conducting periodic audits of corporate security and reporting the findings to the CSEC Audit and Evaluation Committee.

2.7 Director, Corporate Security (DCS)

The Director, Corporate Security (DCS), serves as the Deputy DSO and is accountable to the DG CS Ops for:

- Advising CSEC management on security issues;
- Notifying executives of serious security incidents;
- Managing directly the programs that deliver personnel security, physical, technical, and industrial security, and security policy and education;
- Coordinating with the ITSC on IT security;

Continued on next page

2. CSEC Security Accountabilities, continued

2.7 Director, Corporate Security (DCS) continued

- Ensuring compliance with corporate and government security policies and standards;
- Coordinating cross-functional security issues, such as investigations, risk assessments, corporate security plans and performance reports;
- Investigating internal security incidents and violations, and identifying and recommending corrective action;
- Being the departmental point of contact for external SIGINT-related security incidents;
- Coordinating with the Director, (SIGINT) Requirements, on the management of SIGINT security incidents external to CSEC;
- Coordinating emergency management and business continuity activities in Corporate Security with the Emergency Management Office (EMO); and,
- Maintaining a national inventory for personnel cleared and indoctrinated to SIGINT.

2.8 Director, Information Security (CIO-R)

The Director, Information Security (CIO-R), is accountable to the CIO for:

- Fulfilling the IT Security Coordinator (ITSC) function, as per *MITS*;
- In the role of ITSC, reporting functionally to the CIO and the DSO, on the fulfillment of the following roles:
    - Departmental Information Systems Security Officer (ISSO), as per the *CSSS*; and,
    - Departmental COMSEC Authority (DCA), as per the *COMSEC Material Control Manual (ITSG-10)*.
- Working with the DCS to ensure the integrity of CSEC's security posture, and to provide assurances to the DSO and senior executives.

Continued on next page

2. CSEC Security Accountabilities, continued

2.9 Managers

CSEC Managers are responsible for ensuring the protection of employees and safeguarding the information, assets and services for which they are responsible. With the advice, guidance and support of the DCS, the ITSC, and HR specialists, managers are accountable for:

- Ensuring that security requirements are integrated into business planning, programs, services and other management activities;
- Assessing security risks, formally accepting residual risks or recommending acceptance of residual risks, and periodically reassessing and re-evaluating risks in light of changes to programs, activities or services, and taking corrective action to address identified deficiencies;
- Monitoring the implementation and effectiveness of security controls and reporting accordingly to the DCS or security practitioners, as appropriate;
- Ensuring employees apply effective security practices in day-to-day operations;
- When contracting, identifying security requirements involving access to classified or protected information and assets, and confirming that contractors meet security prerequisites before granting access to such information and assets;
- Ensuring that all activities comply with established security policies, procedures, guidelines and standards; and
- Reporting and taking appropriate administrative action, disciplinary sanctions or remedial action, in cases of contraventions of security policies, procedures, guidelines or standards.

2.10 Group Security Officers (GSOs)

Group Security Officers (GSOs) are designated by, and accountable to, their group Directors for:

- Developing, promoting, coordinating and sustaining effective security practices within their groups;
- Providing first-line security advice to employees and managers in their groups;
- Providing first-line support to Corporate Security in the management of security incidents in their groups; and,
- Liaising with Security Policy and Education.

For more information, see *SEC-104 Group Security Officer Program*.

Continued on next page

2. CSEC Security Accountabilities, continued

2.11 Personnel

All CSEC personnel (*i.e.*, employees, secondees, integrees, contractors, students) are responsible for:

- Safeguarding information and assets under their control whether working on- or off-site;
- Applying security controls related to their area of responsibility to ensure that security requirements are part of their day-to-day processes, practices and program delivery;
- Reporting security incidents through the appropriate channels (GSO, manager, or security specialists) and taking direction from management and security practitioners;
- Maintaining awareness of security concerns and issues to ensure their actions do not compromise departmental security; and,
- Working in a manner that is consistent with CSEC security policies, procedures, guidelines and standards.

2.12 Security Committee (SC)

As a sub-committee of the Executive Committee (ExCom), the CSEC Security Committee (SC) is the senior management forum for:

- Discussing corporate security issues;
- Approving security policies;
- Reviewing results from risk assessments with corporate-wide implications; and,
- Reviewing security plans and performance reports.

An ExCom member chairs the SC and reports to ExCom on SC activities.

For more information, see the *Terms of Reference for the CSEC Security Committee*.

3. Additional Information

3.1 References

SEC-100 refers to the following:

- Treasury Board of Canada Secretariat (TBS), *Policy on Government Security (PGS)*, July 2009
- TBS, *Directive on Departmental Security Management (DDSM)*, July 2009
- TBS, Operational Security Standard on the *Management of Information Technology Security (MITS)*, May 2004
- CSEC, *Canadian SIGINT Security Standards (CSSS)*, March 1995
- CSEC, *IT Security Guidance COMSEC Material Control Manual (ITSG-10)*, July 2006
- Ministerial Directive, *CSE Accountability Framework,* 19 June 2001
- CSEC Legal Services, *CCSE Security Authorities,* 23 December 2004
- CSEC, SEC-104 *Group Security Officer (GSO) Program*, November 2009
- CSEC, SEC-404 *CSE Certification and Accreditation Policy,* June 2005
- CSEC, OPS-5-6 *Providing Access to SIGINT information,* December 2003
- CSEC, OPS-5-7 *ECI Handling Standards,* May 2010
- CSEC, OPS-5-8 *GAMMA Handling Standards*, July 2007

3.2 Annex

Annex 1 of SEC-100 depicts CSEC security roles in chart form.

3.3 Enquiries

Send questions to Corporate Security via ARS.

Annex 1: CSEC Security Roles Matrix

Lead	Shared

(based on TBS *Departmental Directive on Security Management* "security control objectives", plus Operational and Technical Security Standards)

Internal Security Responsibilities	Chief	DC CS	DC SIGINT	DC ITS	CIO	DGAEE	DCS	Managers	Remarks
1. Information assurance		DGPC			ITSC				all personnel support
2. Individual security screening									
3. Physical security									
4. Information technology (IT) security					ITSC				*MITS* sec.9.1
5. Security in contracting		DGFIN							
6. Sharing information and assets with other governments and organizations		DGPC							DCSIGINT, DCITS support
7. Obtaining security services from other organizations		DG CS OPS (DSO)							
8. Security awareness									all personnel support
9. Security training									
10. Security incident management									ITSC, DGHR support
11. Protection of employees from workplace violence		DGHR (OHS)							
12. Security inspections									
13. Administrative investigations related to security incidents									DGHR, Managers support
14. Security in emergency and increased threat situations									
15. Emergency and business continuity planning		DG CS OPS (DSO)							through Director Program Management
16. Monitoring and oversight									
17. Senior Indoctrinated Official (SIO)									*CSSS* sec 2.2.1
18. COMINT Control Officer (COMCO)									*CSSS* sec 2.2.2
19. Information Systems Security Officer					ITSC				*CSSS* sec 2.2.3
20. Departmental COMSEC Authority					ITSC				*ITSG-10* sec 3.2.1
21. COMSEC Custodian				Dir T					*MITS* sec 9.9

Effective date 1 January 2006; amended 19 December 2013

SEC-201 – Polygraph Testing Policy

1. Introduction

1.1 Objectives

- To provide a mechanism for assessing an individual's loyalty to Canada, thereby reducing potential risks to national security.
- To establish a framework within which polygraph testing will be administered as part of the CSE security screening process.

1.2 Authority

The authorization for the polygraph testing of individuals derives from the *Ministerial Directive (MD) – Communications Security Establishment: Polygraph Testing* (1 June 2005).

1.3 Context

Polygraph testing is one of several tools used during the security screening process to help determine whether an individual represents a security risk to CSE based on his or her loyalty to Canada, and therefore is unsuitable to perform the duties of a position within, or render a service to, CSE.

1.4 Application

This policy applies to all individuals permitted to work at or represent CSE, including:

- term and indeterminate employees
- contractors
- students
- Canadian secondees (including Department of National Defence (DND) personnel), and
- Department of Justice (DoJ) personnel.

2. Policy

2.1 Principles

- CSE employs various security measures to protect its information, assets, operations, and critically important partnerships. One such measure is polygraph testing in accordance with the 2005 MD.
- A polygraph test
  - is not the sole determinant in CSE's security screening and selection process
  - relates only to the individual's loyalty to Canada, and
  - may be used only as an investigative tool.

s.15(1) - DEF

- CSE implements and manages its polygraph program in compliance with the *Canadian Charter of Rights and Freedoms*, the *Canadian Human Rights Act*, the *Privacy Act*, and other relevant legislation and existing government policies, as well as relevant human resources policies that are common to all Government of Canada organizations.
- CSE rigorously manages the program, ensuring professional test administration; strict procedures and quality assurance; tightly controlled dissemination, storage, retention and destruction of information resulting from the tests; and periodic review.

2.2 Mandatory testing

Polygraph testing is mandatory for individuals at CSE who require, or who already hold, a Top Secret SIGINT Information Access (TS/SIA) security clearance,[1] **and** who fall into one of the following categories:

- Candidates being considered for new employment, whether indeterminate, term, secondee or student
- All employees, secondees and students hired at each five-year security clearance update
- All applicants being considered for any contractual arrangements at CSE; and thereafter, all contractors at each five-year security clearance update

Continued on next page

2. Policy, continued

2.2 Mandatory testing (continued)

- Any individual, irrespective of when he or she joined CSE, who assumes a designated sensitive function (see Annex 1), unless they have had a polygraph test within five years of assuming that function
- Employees slated for integration within other government departments or agencies that utilize polygraph testing, *e.g.*, CSIS
- DoJ employees assigned to the CSE Legal Services Unit at the time of joining and at each five-year security clearance update
- Any former employee, secondee, student, contractor or DoJ personnel, being considered for re-employment by CSE who has been absent for more than 12 months, as well any "candidate-in-waiting" (*i.e.*, any individual from the list of qualified cleared applicants) who has not received a letter of offer within 12 months of his or her original polygraph test, **unless** the following conditions are met:

s.15(1) - DEF

–

–

–

  - ▪
  - ▪

2.4

Employees hired unless they assume a designated sensitive function and have not had a polygraph test within five years of assuming that function.

Continued on next page

[2] "

[3] Section 2 of the *CSIS Act*.

2. Policy, continued

2.5 Voluntary testing

Any individual working at CSE may volunteer to take a polygraph test in the following scenarios.

Scenario	Rationale
Security investigation	An individual may volunteer to undergo a polygraph test when the test may clarify issues and assist in the resolution of a security investigation. Examples of this scenario are when • an individual's security clearance is under review for cause, or • there is reason to believe that his or her actions may have seriously compromised national security or indicated the need to reassess loyalty to Canada, in accordance with *SEC-101 Security Incidents and Investigations*.
High-risk personal travel	Individuals wishing to engage in high-risk personal travel may volunteer for a polygraph test if they believe it would further mitigate the risk of such travel.

2.6 Notice

CSE will

- give prior notice to all individuals requiring polygraph testing
- inform individuals that a polygraph test is a requirement of the CSE security screening process and that a refusal to comply with this requirement will automatically result in the discontinuation of that process, and
- inform individuals who are subjects of an internal investigation that no adverse inference will be made if they refuse to undergo a polygraph examination.

2.7 Consent

All individuals undergoing polygraph testing must first read and sign the *CSE Consent Form to Undergo a Polygraph Examination*. This form includes permission for the use of electronic video and/or audio recording during the polygraph test.

Continued on next page

2. Policy, continued

2.8 Conduct of testing

CSE conducts polygraph tests in accordance with the following.

Issue	Policy
Scope	• The polygraph test must relate only to the individual's loyalty to Canada, as reflected in the questions in the polygraph test report. • In situations involving an internal investigation, the questions must refer specifically to the matter under investigation. •
Examiner	Only a skilled and accredited polygraph examiner, approved by and under the supervision of the CSE Supervisor, Polygraph Assessment Services, will conduct the tests.
Quality control	All polygraph tests will be reviewed by the Supervisor, Polygraph Assessment Services, or a senior Polygraphist. In addition, a random sample of all polygraph tests will be subject to the quality-control process of an external accredited polygraph specialist.
Official Languages	The polygraph test must be conducted in the official language of the individual's choice.
Individuals with special needs	Should an individual have special needs or requirements as a result of functional limitations, arrangements will be made to accommodate their needs.

s.15(1) - DEF

2.9 Measurement of Potential Risk

Polygraph test results will include a measurement of potential risk to CSE operations.

Risk measurements are categorized in five levels: low, low to moderate, moderate, moderate to high, and high, based on test results and information as it relates to loyalty.

Continued on next page

2. Policy, continued

2.9 Measurement of Potential Risk (continued)

The Supervisor, Polygraph Assessment Services, will recommend that the selection screening process continue for mandatory polygraph test results

2.10 Post-test processing

After a test has been independently reviewed and quality controlled, the next steps are as follows.

If the results indicate…	Then…
no security concern	Supervisor, Polygraph Assessment Services, informs the Personnel Security Officer
a possible security concern	• Polygraph examiner will – offer the individual the opportunity to discuss and explain any anomalous response, and – report the results to the Supervisor, Polygraph Assessment Services, and/or the Manager, Personnel Security • Supervisor, Polygraph Assessment Services and/or the Manager, Personnel Security, will inform the Personnel Security Officer and decide whether a follow-up interview is required • Manager, Personnel Security, may inform the appropriate first-level review body (*i.e.*, the Hiring Panel or Contracting Panel), and the Director, Corporate Security (DCS) • DCS may inform the Departmental Security Officer (DSO) and the Deputy Chief, Corporate Services (DCCS)

s.15(1) - DEF

Continued on next page

2. Policy, continued

2.11 Records

- Only the Manager, Personnel Security and the Polygraph Assessment Services Unit may access the polygraph files in storage at CSE.
- The CCSE, DSO, DCS, the Manager, Personnel Security, and others specifically requested and authorized by the CCSE to conduct an investigation, may receive access to polygraph files on a restricted, "as needed" basis.
- The polygraph file of a CSE employee or contractor will be retained under appropriate security measures by CSE Records Services for as long as the individual is employed or under contract at CSE, and for an additional period of two years after the last administrative action. At that point, the polygraph file will be destroyed.
- The polygraph file of an individual not hired or awarded a contract at CSE will be retained under appropriate security measures by CSE Records Services for two years after the last administrative action. At that point, the polygraph file will be destroyed.
- Irrespective of the storage location of CSE polygraph files, the Polygraph Assessment Services Unit retains ownership of the files, which normally include:

s.15(1) - DEF

3. Accountability

3.1 Roles and responsibilities

The following table outlines roles and responsibilities under this policy.

Who	Responsibility
Chief, CSE (CCSE)	• Is accountable to the Minister of National Defence for the management of polygraph testing as required by the Ministerial Directive of 1 June 2005 • Renders the final decision on any problematic case reviewed and referred by the DSO • Approves amendments to the list of designated sensitive functions that require mandatory polygraph testing
Departmental Security Officer (DSO) s.15(1) - DEF	• May inform the Deputy Chief, Corporate Services of any problematic cases, • Reviews and refers problematic cases to the CCSE for final decision
Director, Corporate Security (DCS)	• Ensures that CSE's Polygraph Program is managed in a way that is consistent with the MD, this policy and all other related policies, procedures and guidelines
Manager, Personnel Security	• Under the direction of the DCS, ensures that CSE's Polygraph Program is administered in compliance with the MD, this policy and all other related policies, including periodic review of the program • Determines the course of action if there are following a problematic polygraph test result; this per SEC-101

Continued on next page

3. Accountability, continued

3.1 Roles and responsibilities (continued)

Who	Responsibility
Supervisor, Polygraph Assessment Services	• Administers, under the direction of the Manager, Personnel Security, CSE's Polygraph Program in accordance with this policy and all applicable professional standards • Ensures that CSE polygraph examiners are trained to conduct and analyze polygraph tests, and are members in good standing with the American Polygraph Association and abide by its code of conduct and ethics

3.2 Performance measures

In accordance with the Ministerial Directive, CSE will provide the Minister of National Defence with an assessment of the use of the polygraph at CSE on a yearly basis in CSE's Annual Report.

3.3 Enquiries

Send questions to Corporate Security via ARS.

Annex 1 – Designated Sensitive Functions

A1.1 Functions

The following are designated sensitive functions*:

- CCSE and all positions directly reporting to the CCSE
- Foreign postings such as, but not limited to, Canadian Special Liaison Offices (CANSLOs), secondments, integrations and temporary duties in excess of six months
- Executive Committee (ExCom) support functions, as identified by the responsible ExCom Member and designated by the CCSE
- Functions involving access to certain Exceptionally Controlled Information (ECI) compartments, as identified by the responsible ExCom Member and designated by the CCSE;
- Certain functions requiring account administration privileges, as identified by the responsible ExCom Member and designated by the CCSE;
- Certain personnel and physical security functions as identified by the responsible ExCom Member and designated by the CCSE; and
- Any other functions with access to highly sensitive information or involving highly sensitive operations, as deemed appropriate by the CCSE.

* **Note**: Any assignment, including acting situations, in a designated sensitive function for greater than six months will require a polygraph test.

CONFIDENTIAL
Published on Communications Security Establishment

About the Polygraph Testing Policy

s.15(1) - DEF

By
Created 2011-Apr-27 15:43
Quick Reference type: General Reference

1. Why did the Minister of National Defence direct that CSE's polygraph testing program be expanded to include five-year updates for those hired

The Minister of National Defence is accountable to Parliament for CSE and, as such, is rightly concerned with the integrity and security of our operations, especially our most sensitive functions. Our increasingly important role in contributing to Canada's national security has come as a result of some critical new authorities. As a result, it has become more important to ensure that CSE reduce the risk of a security breach that could jeopardize our mission or those of our partners. The expanded polygraph testing policy brings us in line with other security and intelligence agencies.

The Policy on Government Security requires security clearance updates for employees every five years regardless of length of employment or job performance. Ongoing security clearance management is a feature of working at CSE. We have personnel security updates and a security awareness program for all employees because any number of life-changing events might affect an individual's suitability to hold a Top Secret/SIGINT Information Access (TS/SIA) clearance. CSE must ensure that its highly sensitive information and operations receive the greatest measure of protection from compromise.

2. What measures are in place to protect my privacy?

In the course of the security screening process, the employee's consent is required before a personal background check or a polygraph test can proceed. Like all of CSE's operations, the polygraph program must comply with the Privacy Act. Polygraph files are strictly compartmented and every measure is taken to ensure confidentiality. As per the 2003 Ministerial Directive on polygraph testing, an annual report on the conduct of CSE's polygraph testing program is prepared for the Minister each year. An audit conducted by the Director General of Audit & Evaluation in 2005 found the polygraph program to be well managed and compliant with all relevant legislation.

3. Who has access to my polygraph results?

CSE maintains strict controls on the protection of personal information as required by the Privacy Act. A copy of the polygraph report, summarizing the outcome, is kept on your security file. Polygraph results are separately compartmented within the security file system, under the control of the Polygraph Assessment Services Supervisor. There is a very short list of individuals in the chain of command who can have access to the file on a restricted, need-to-know basis in the course of a security investigation:

1. Manager, Personnel Security
2. Director, Corporate Security (DCS)
3. Departmental Security Officer (DSO)
4. Deputy Chief Corporate Services (DCCS)
5. Chief of CSE (CCSE)
6. Anyone else specifically requested and authorized by CCSE in order to conduct an investigation.

4. How long are my polygraph results kept on file?

Polygraph files are kept for as long as you are employed at CSE in any capacity and for two years after you leave. After that, they are destroyed in accordance with Government of Canada legislation and policy regarding retention and disposal.

5. Can I request to see my polygraph file?

You may request an informal review of your file with the polygraph examiner. To receive a record of your polygraph results to keep for yourself, you would have to submit a request under the Privacy Act.

For more information on the polygraph testing program, see:

- About the Polygraph Test Procedures
- About Designated Positions
- SEC-201 Polygraph Testing Policy
- SEC-201-1 Polygraph Designation Guide for Managers
- Polygraph Decision Chart

If you have any questions, please submit them to Corporate Security using the Service Catalogue in the Employee Self-Service (ESS) Portal or HP Service Manager (HPSM).

Corporate Security Directorate (S)
Personnel Security (S2)
Security Policy and Education (S3)
Corporate Security Policy Program
Group Security Officer (GSO) Program
Polygraph Assessment
Security Screening and Clearance Updates
Corporate Services Operations (CSOPS)
Corporate Services (DCCS)
Psychological Assessment Services

s.15(1) - DEF

Source URL: 'about-polygraph-testing-policy
CONFIDENTIAL

CONFIDENTIAL
Published on Communications Security Establishment (

About the Polygraph Test Procedures

s.15(1) - DEF

By
Created 2011-Apr-27 16:11
Quick Reference type: General Reference

1. Is the polygraph test conducted by the same person who does the security interview?

No, the polygraph test is administered by a trained polygraph examiner who is authorized to conduct and analyze polygraph tests after graduation from an accredited polygraph institute. CSE's polygraph examiners are required to be members of the American Polygraph Association and to follow its code of conduct and ethics and meet its continuing education standards.

2. What kinds of questions are asked during the polygraph test?

3. Does the polygraph examination look at personal lifestyle?

No, the test is designed to focus and report on loyalty-related issues only, including such areas as:

These questions can involve asking about personal history or past activities but only for the purpose of determining if the person's loyalty has been compromised.

4. If the polygraph examiner sees a problematic test result while I'm undergoing the polygraph test, will I be told and given a chance to explain?

5. What happens if I refuse to answer a question?

The polygraph test is a collaborative process and, through discussion with you, However, if you are unable to provide adequate information, the screening and staffing process may be terminated.

6. Will I be told the results of my polygraph test?

Yes, as soon as the test is complete, the polygraph examiner will tell you what your results are. You must keep in mind, however, that the examiner's opinion isn't considered final until the results have been reviewed and quality-controlled by another accredited polygraph examiner.

7. What kind of quality control applies to polygraph testing and results analysis?

All aspects of CSE's polygraph testing program are quality-controlled. Polygraph test results are reviewed by another trained and accredited polygraph examiner before the results are considered final.

8. Can I lose my security clearance if my polygraph test has a negative result?

No, the polygraph is never used as the sole determinant in the security screening process — there are always other corroborative screening measures used. If security-related concerns arise as a result of the polygraph test, every attempt would be made to resolve them with you through an interview Personnel Security is here to help employees maintain their security clearances.

For more information on the polygraph testing program, see:

s.15(1) - DEF

- About the Polygraph Testing Policy
- About Designated Positions
- SEC-201 Polygraph Testing Policy
- SEC-201-1 Polygraph Designation Guide for Managers
- Polygraph Decision Chart

If you have any questions, please submit them to Corporate Security using the Service Catalogue in the Employee Self-Service (ESS) Portal or HP Service Manager (HPSM).

Corporate Security Directorate (S)
Personnel Security (S2)
Security Policy and Education (S3)
Corporate Security Policy Program
Group Security Officer (GSO) Program
Polygraph Assessment
Security Screening and Clearance Updates
Corporate Services Operations (CSOPS)
Corporate Services (DCCS)
Psychological Assessment Services

Source URL: about-polygraph-test-procedures
CONFIDENTIAL

CONFIDENTIAL
Published on Communications Security Establishment

About Designated Positions

By
Created 2011-Apr-27 12:42
Quick Reference type: General Reference

s.15(1) - DEF

1. The policy states that the Chief can add to the list of designated sensitive functions, so will the list expand to include more positions?

As our operations continue to evolve in the face of changing technologies and a changing global environment, it is possible that more functions in CSE might be designated. Similarly, functions could be undesignated if their sensitivity changes.

2. I've been at CSE just over a year and underwent a polygraph test as part of the hiring process. If I move to a designated position, do I have to be tested again?

No, you would not have to undergo another polygraph because your polygraph test results are less than five years old.

3. I joined CSE and am not polygraphed as part of my five year security clearance update. If I undergo a polygraph test to move into a designated sensitive position, do I then have to be tested every five years when my security clearance is updated?

Also, if you apply to work in another designated position in the future, you will not have to be re-tested if it has been less than five years since your last polygraph test.

4. Which functions are designated as requiring polygraph testing?

The Ministerial Directive identified two categories of designation — mandatory and discretionary. Mandatory functions that must be polygraphed include:

- CCSE and all positions reporting directly to the CCSE
- foreign postings (e.g., the Canadian Special Liaison Offices (CANSLOs), secondments, integrations and temporary duties in excess of six months)

Discretionary functions must also be polygraphed but CCSE was given the discretion to designate which positions within those functions are the most sensitive. These categories include functions that:

- provide administrative support to the Executive Committee (including acting assignments lasting more than six months)
- have access to certain Exceptionally Controlled Information (ECI)
- have administrative account privileges.
- have personnel and physical security functions
- involve highly sensitive information or operations

5. How many positions at CSE are designated?

s.15(1) - DEF

of the positions at CSE are designated as requiring polygraph testing. For security reasons, the complete list is not being posted — making available a compilation of our most sensitive positions would pose an unnecessary security risk.

6. What criteria were used to designate positions for polygraph testing?

Criteria were established to assess the sensitivity of positions in terms of the degree of access that an individual requires to CSE's most sensitive information and operations in order to fulfill part or all of their day-to-day responsibilities. These criteria were developed in consultation with senior management and then approved by executive levels.

Category	Criteria
ExCom support	• Degree of access to ExCom deliberations, decisions, and documentation and other highly sensitive information.
ECI Access	• The degree of access to the most sensitive operational details
Account Administration	• Privileged access to CSE networks, systems, infrastructure, components, applications, and content. Examples include system, database, and application administration.
Personnel and Physical Security	• Knowledge of physical or personnel security measures that
Highly Sensitive Information Access	• The degree of access to highly sensitive information, including CSE's corporate document repository.

For more information on the polygraph testing program, see:

- About the Polygraph Testing Policy
- About the Polygraph Test Procedures
- SEC-201 Polygraph Testing Policy
- SEC-201-1 Polygraph Designation Guide for Managers
- Polygraph Decision Chart

If you have any questions, please submit them to Corporate Security using the Service Catalogue in the Employee Self-Service (ESS) Portal or HP Service Manager (HPSM).

Corporate Security Directorate (S)
Personnel Security (S2)
Security Policy and Education (S3)
Corporate Security Policy Program
Group Security Officer (GSO) Program
Polygraph Assessment
Security Screening and Clearance Updates
Corporate Services Operations (CSOPS)
Corporate Services (DCCS)

Source URL: 'about-designated-positions
CONFIDENTIAL

s.15(1) - DEF

Effective Date: 10 April 2006; amended 19 December 2013

SEC-201-1 – Polygraph Designation Guide for Managers

1. Designated positions under SEC-201

CSE's Polygraph Testing Policy was updated effective to reflect the 2005 Ministerial Directive (MD), which

- designates certain positions that require *mandatory* polygraph testing, and
- identifies general categories of functions for which the Chief, CSE (CCSE), has the *discretion* to designate particular positions for polygraph testing.

Designation Requirement	Positions/Functions
Mandatory	• CCSE and all positions directly reporting to the CCSE • Foreign postings, integrations, and temporary duties in excess of six months • Secondments and temporary duties with Canadian departments and agencies that also utilize polygraph testing
Discretionary	• Executive Committee (ExCom) support • Access to Exceptionally Controlled Information (ECI) • Account administration • Personnel and Physical Security functions • Highly sensitive information access

2. Designation criteria

Criteria are used to assess positions for polygraph designation within each of the discretionary categories. The criteria and the senior manager responsible for each category are as follows:

s.15(1) - DEF

Category	Criteria	Senior Manager
ExCom Support	The degree of access* to ExCom deliberations, decisions, documentation and other highly sensitive information.	Respective ExCom member
ECI Access	The degree of access* to the most sensitive operational details	Director General, Access
Account Administration	Privileged access to CSE networks, systems, infrastructure, components, applications, and content (examples include system, database, and application administration).	Respective ExCom member
Personnel and Physical Security Functions	Knowledge of physical or personnel security measures that	Director, Corporate Security
Highly Sensitive Information Access	The degree of access* to highly sensitive information, including CSE's corporate document repository.	Director, Information Management (CIO-E)

* Normally, the "degree of access" that would warrant a designation is access that an individual requires in order to fulfill part or all of his or her day-to-day responsibilities. Access on an exceptional basis — for example, responding to emergency situations, a temporary change in responsibilities (*i.e.*, normally assignments less than six months in duration), etc. — generally would **not** warrant a polygraph designation.

3. New, cloned, or re-classified positions

A newly created, cloned, or re-classified position will be designated as requiring polygraph testing **if** it falls into

- one of the *mandatory* categories designated in the policy, **or**
- one of the *discretionary* categories **and** meets the designation criteria used to assess the sensitivity of positions in that category.

4. Managerial responsibility

When creating, cloning, or re-classifying a position, managers must assess whether the position should be designated as having a polygraph requirement before completing the Human Resources Services Request (HRSR) form.

5. Procedures for assessing positions

Managers are to follow these steps when assessing whether a position should be designated for polygraph testing:

Step	Action
1	*Does the position fall within one of the **mandatory** categories specified in the* Polygraph Testing Policy*?* • If "**no**", proceed to Step 2. • If "**yes**" - enter "**Proposed**" in the HRSR form, identify the category the position falls under, and complete the remainder of the form, - e-mail the HRSR form to your DG to obtain his/her approval, and - once approved, forward the HRSR form **and** the DG's approval to HR Service Request.
2	*Does the position fall within one of the **discretionary** categories specified in the policy?* • If "**no**", enter "**Non-Applicable**" in the HRSR form, complete the remainder of the form, and e-mail it to HR Service Request. • If "**yes**", proceed to Step 3.

Continued on next page

5. Procedures for assessing positions (continued)

Step	Action
3	*Does the position meet the **designation criteria** for that category?* • If "**yes**" or **unsure**, consult with the senior manager responsible for the criteria governing that category (see section 3) and proceed to Step 4. • If "**no**", enter "**Non-Applicable**" in the HRSR form, complete the remainder of the form, and e-mail it to HR Service Request.
4	*Does the senior manager responsible for that category **agree** that the position meets the designation criteria?* • If "**no**", enter "**Non-Applicable**" in the HRSR form, complete the remainder of the form, and e-mail it to the HR Service Request. • If "**yes**" - enter "**Proposed**" in the HRSR form, identify the category the position falls under, and complete the remainder of the form - email the HRSR form to your DG to obtain his/her approval, and - once approved, forward the HRSR form and the DG's approval to HR Service Request.

6. Approval process

The Corporate Security Senior Policy Analyst will

- forward all positions proposed for polygraph designation through the Director, Corporate Security, to CCSE for approval
- notify the respective hiring manager of the decision, and
- notify Staffing so that the designation status of the position and effective date can be entered in PeopleSoft.

7. De-designating positions

The rationale for designating a position within the discretionary categories may change (*e.g.*, different duties, disestablishment of ECIs), and no longer meet the designation criteria. Managers **must** ensure that the polygraph designation status of positions in their areas remains current.

Continued on next page

7. De-designating positions (continued)

If a manager believes a position should be removed from the list of designated positions, the following de-designation procedures apply:

Step	Action
1	Obtain the agreement of the senior manager responsible for the designation criteria within the applicable category • If "**no**", do not change the designation status of the position. • If "**yes**", obtain the agreement of your DG to de-designate the position.
2	Send a proposal to the Corporate Security Senior Policy Analyst to de-designate the position • providing the rationale for the change, and • indicating the agreement of both the senior manager responsible for that category and your DG.

The Corporate Security Senior Policy Analyst will

- forward the proposal, through the Director, Corporate Security, to CCSE for approval
- notify the respective hiring manager of the decision, and
- notify Staffing so that the designation status of the position and effective date can be entered in PeopleSoft.

8. Abolishing designated positions

When abolishing a designated position, managers must (in addition to submitting the HRSR form to HR Service Request) separately notify the Corporate Security of the abolishment via the ARS system ("Corporate Security Policy"), so that Corporate Security can maintain a current record of CSE's polygraph designated positions.

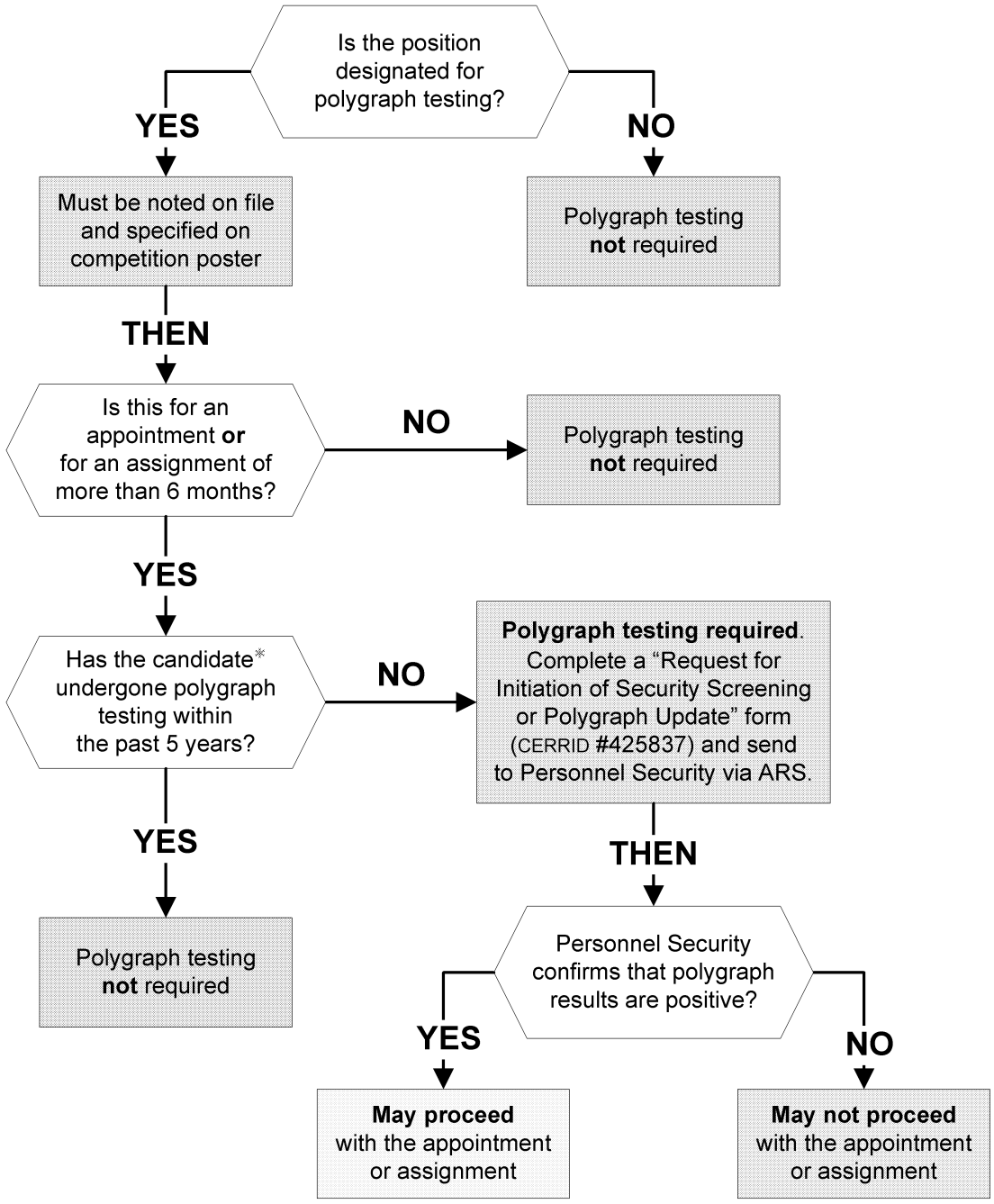
9. Further information

For more information, managers can

- consult CSE's *Polygraph Testing Policy* (SEC-201)
- send questions to Corporate Security via ARS.

Polygraph Decision Chart

Determining whether polygraph testing is required for an internal staffing process



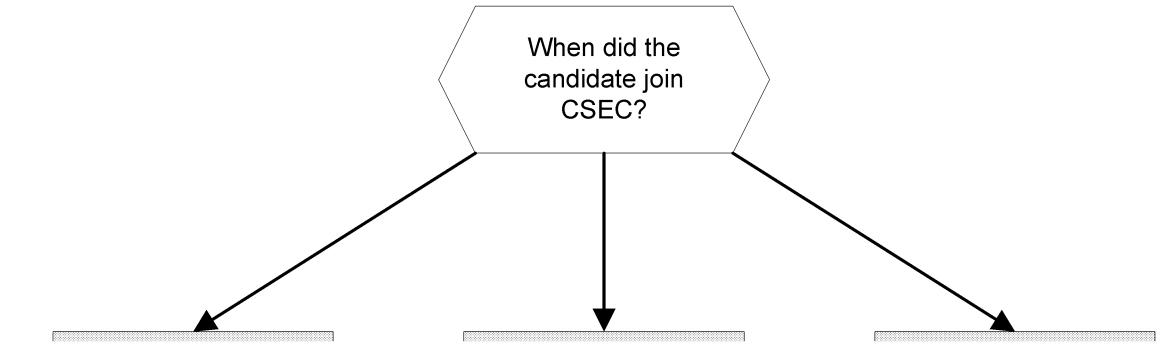
* *Only the **first** successful candidate is to be sent for polygraph testing **unless** the intent is to appoint more than one candidate.*

CERRID #683941 (June 2011)

Canada

Polygraph Scenario Chart

Polygraph testing requirements based on when the candidate joined CSEC



The candidate ...

-
-
- **does** require polygraph testing if appointed to a designated position

The candidate ...

- **did** undergo polygraph testing when hired
-
- **does** require polygraph testing if appointed to a designated position **UNLESS** their original polygraph test results are **less than** 5 years old

The candidate ...

- **did** undergo polygraph testing when hired
- **does** undergo polygraph testing as part of their five-year updates
- **does not** require polygraph testing if appointed to a designated position **UNLESS** their most recent polygraph test results are **more than** 5 years old

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Human Resources

Effective Date: February 17, 2011

CERRID #739611

HRH-18 – POLICY ON PSYCHOLOGICAL ASSESSMENT SERVICES

1. Objective

1.1 Objective

To explain the circumstances and situations when psychological assessments will be administered either in a mandatory or voluntary capacity.

2. Context

2.1 Context

- CSEC utilizes various measures and tools to protect its operations, assets and critically important partnerships;
- As a result of a 2002 Excom decision, psychological testing was implemented as one of the tools used in the selection screening process in February 2003;
- Psychological assessments have proven to be a valuable means of assessing the reliability of individuals and providing an indication of either current or potential behaviour that may significantly affect an individual's performance at work and/or pose a risk to CSEC operations;
- Psychological assessments have also been beneficial in determining an individual's psychological readiness, a critical factor when undertaking higher risk or stressful assignments.

3. Application

3.1 Application

This policy shall apply to all individuals being considered for employment within CSEC, for a contract, or to represent CSEC and includes the following:

- indeterminate and determinate employees;
- students;
- contractors[1];
- Canadian secondees, excluding secondees from the Department of Justice Canada and National Defence.

4. Authority

4.1 Authority

This policy has been developed in accordance with the Instrument of Delegation of Human Resources Management Authorities.

5. Policy

5.1 Principles

Psychological assessments will be performed in conjunction with the various other assessment measures and tools in order to evaluate an individual's suitability, reliability and psychological readiness in relation to the performance of duties;

A psychological assessment will not be the sole determinant in either CSEC's selection screening process or in situations when an employee's performance of their current or future task specific duties could pose a risk to CSEC's operations;

Psychological assessments will only be administered to individuals who have read and signed the CSEC *Consent Form for Psychological Assessment;*

Psychological assessments, interviews and the interpretation of the psychological assessment results will only be carried out by a registered psychologist recognized by a Psychological Order or by an Association of any Canadian province. Psychological assessments will be conducted in compliance with the Canadian Charter of Rights and Freedoms, the Canadian Human Rights Act, the Privacy Act and other relevant legislation and policies.

[1] Definitions - Section 11.1

6. Policy Requirements

6.1 Categories for Mandatory Psychological Assessments

A psychological assessment is mandatory for individuals who require, or who may already possess a Top Secret clearance and a SIGINT Information Access indoctrination and who fall into one of the following categories:

- individuals being considered for employment at CSEC for the first time, secondees and students including those whose previous CSEC psychological assessment results exceed the validity period[2];
- students when a change in their employment status, such as becoming an indeterminate employee, is being considered;
- former students who have been absent from CSEC for more than twelve (12) months, being considered for a new work term;

s.15(1) - DEF

-
- employees being considered to assume a designated sensitive function[3] after the effective date of this policy unless they have had a psychological assessment within the past five (5) years of assuming the function;
- former employees, secondees or contractors being considered by CSEC for re-employment or a contract who have been absent from CSEC for more than twelve (12) months if a letter of offer or contract has not been issued and:
    - they have not been assessed by CSEC Psychological Assessment Services in the past five (5) years;
    - a review of their security file supports the need for a psychological assessment, if there are concerns about any of the following elements:
        -
        -

Continued on next page

[2] Definitions – Section 11.7
[3] Section 11.3
[4] *CSIS Act* – Section 2

6. Policy Requirements, Continued

6.1 Categories for Mandatory Psychological Assessments (continued)

s.15(1) - DEF

6.2 Voluntary Psychological Assessments

When an employee's behavior causes concern of a potential risk for CSEC, consultation and discussion regarding the concerns will take place between the Manager, Personnel Security, the Manager, HR Labour Relations and Negotiation, the Head, Psychological Assessment Services, the employee, the employee's manager, the employee and, if desired by the employee, a person of their choosing to be in attendance. The employee may choose to undergo psychological assessment however the assessment will only be administered by the Psychological Assessment Services team with the employee's agreement and written consent.

Should the employee choose to have a psychological assessment performed by a mental health professional external to CSEC, the Head of Psychological Assessment Services may request a copy of the report from the external mental health professional. This report can only be obtained with an authorization of divulgation of information signed by the employee. In these situations, the Head. Psychological Assessment Services will provide guidance with respect to the results of the external report to the parties involved.

The results of voluntary psychological assessments, will be strictly confined and will only be shared with the Manager, Personnel Security, the Manager HR Labour Relations and Negotiations, the Director General Human Resources (DGHR), the Director of Corporate Security and any other individuals who are directly involved in any decision regarding the employee's psychological readiness or suitability to perform their duties. If required, a member of the Directorate of Legal Services may be included.

Continued on next page

[5] Any individual considered for contracts at CSEC could be required to undergo psychological assessment if requested by Personnel Security.

6. Policy Requirements, Continued

6.3 Consent

All individuals undergoing a psychological assessment must first read and sign the CSEC *Consent Form for Psychological Assessment*.

6.4 Conduct of the Psychological Assessment

- Within CSEC, only a psychologist recognized by a Psychological Order or an Association of any Canadian province may conduct a psychological interview and interpret the results of a psychological test.
- The psychological assessment will be administered in the individual's official language of choice;
- Individuals with special needs or requirements as a result of functional limitations should identify their needs prior to the assessment so that the appropriate accommodation can be arranged.

6.5 Measurement of Potential Risk

- Psychological assessment results will include a measurement of potential risk. The measurement of potential risk linked with the psychological assessment results can provide a valuable indication of factors that could significantly affect an individual's performance at work and/or pose a risk to CSEC operations.
- Risk measurements are categorized in five (5) levels: low, low to moderate, moderate, moderate to high and high.

s.15(1) - DEF

- The Head, Psychological Assessment Services will recommend that the selection screening process continue for mandatory psychological assessments results

6.6 Records

Every psychological assessment file contains general documentation as well as raw data. Raw data, such as test scores and interview notes, can only be interpreted by a registered psychologist and will be kept in a sealed envelope within the psychological assessment file.

Continued on next page

6. Policy Requirements, Continued

6.6 Records (continued)

Access to the psychological assessment files is restricted to members of the CSEC Psychological Assessment Services Team. The protection of the information contained therein will be carried out in accordance with Access to Information and Privacy Laws, as well as all applicable standards of confidentiality contained in the Ethics Code and Code of Conduct of the relevant Psychological Order or Association.
In the event of an Access to Information and Privacy (ATIP) request, the right of access of the psychological assessment file to the individual making the request may be exercised using two methods; the release of the general documentation portion to the individual, and the opportunity of the individual to examine the raw data portion rather than its release. The right of access to the raw data portion must be exercised in the presence of a member of the CSEC Psychological Assessment Services Team and a mental health professional chosen by the individual, if the individual requests a psychologist of his/her choice.

Pursuant to Section 25 and 28 of the Privacy Act, access to either the entire or part of the psychological assessment file may be refused in cases where the disclosure of which could reasonably be expected to threaten the safety of individuals, or not in the best interest of the individual making the request for access.

7.1 Director General, Human Resources (DGHR)

The DGHR will ensure that Psychological Assessment Services are managed and administered in a manner that respects CSEC values.

7.2 Head, Psychological Assessment Services

The Head, Psychological Assessment Services will ensure that psychological assessments are administered in accordance with this policy, all applicable professional standards and relevant legislation.

8.1 Performance Measures

For quality control purposes, the Head, Psychological Assessment Services will review the following psychological assessments:

-
- twenty-five percent (25%) of all assessments, on a random basis.

s.15(1) - DEF

9. References

9.1 References

- *Canadian Charter of Rights and Freedoms*
- *Canadian Human Rights Act*
- *Privacy Act*
- *Access to Information Act*
- SEC 201 Polygraph Testing Policy

10. Enquiries

10.1 Application

Enquiries relating to the application of this policy should be directed to the Head, Psychological Assessment Services.

10.2 Interpretation

Enquiries relating to the interpretation of this policy should be directed to an HR Corporate Policy Advisor.

11. Definitions (for the purposes of this policy)

11.1 Contractor

Refers to a person who has entered into a contract or arrangement with Her Majesty in right of Canada, a department, board or agency of the Government of Canada or a Crown corporation as defined in subsection 83(1) of the *Financial Administration Act*, and includes an employee of the person, a subcontractor of the person and an employee of the subcontractor.

11.2 Designated Sensitive Functions[6]

Refers to:

- Chief, Communications Security Establishment Canada (CCSEC) and all functions directly reporting to the CCSEC;
- foreign postings such as, but not limited to, Canadian Special Liaison Offices (CANSLOs), secondments, integrations and temporary duties in excess of six (6) months;
- Executive Committee support functions as specified by Executive Committee members;
- functions involving access to certain Exceptionally Controlled Information compartments, as designated by the CCSEC;
- certain functions requiring administrative account privileges, as designated by the CCSEC;
- certain personnel and physical security functions, as designated by the CCSEC;
- any other functions with access to highly sensitive information or involving highly sensitive operations, as deemed appropriate by the CCSEC.

Note: Any assignment or acting appointment to a designated function for greater than six (6) months will require a psychological assessment.

11.3 High Risk Area

Refers to an area which has been designated as high-risk by Foreign Affairs Canada (FAC) (i.e. an area for which FAC has issued a travel warning). For more information on the high-risk areas defined by FAC, consult the Consular Affairs website at http://www.voyage.gc.ca/.

11.4 Potential Risk

Refers to current or potential issues which could be detrimental to the individual, to their performance of duties, and/or to CSEC or to National Security.

Continued on next page

[6] Sec 201 Polygraph Testing Policy

11. Definitions (for the purposes of this policy) Continued

11.5 Psychological Assessment	Refers to the gathering of psychological data for the purposes of performing a psychological evaluation, through the use of tests, an interview, a case history and behavioral observation.
11.6 Raw Data	Refers to the test scores and interview notes taken by the psychologist.
11.7 Validity Period	Refers to the twelve (12) month period that CSEC psychological assessment results are considered to be valid.

Effective date: 24 October 2007; amended 26 February 2014

SEC-103 – Protecting and Classifying Information

1. Introduction

POLICY UPDATES

This version of SEC-103 reflects the following developments that have unfolded since the 2007 release of the policy:

- Replacement of the *Government Security Policy* (GSP) with the *Policy on Government Security* (PGS);
- Publication of the new *Canadian SIGINT Security Standards* (CSSS-100);
- Elimination of "COMINT" as a security marking, and its replacement with "SI" (Special Intelligence); and,
- Implementation of the CERRID information management system at CSE.

1.1 Objectives

SEC-103:

- explains the basis for information protection and classification;
- provides an overview of the security marking system; and,
- enables CSE personnel to select appropriate security markings.

1.2 Authority

Treasury Board Secretariat *Policy on Government Security* (PGS), 2009, section 5.2:

> "The expected results of this policy are [that] information, assets, and services are safeguarded from compromise".

Continued on next page

1. Introduction, continued

1.3 Application

These procedures apply to all CSE personnel and any other parties acting under CSE's authority, including students, secondees, integrees, and contractors.

An important aspect of this policy's application is that originators are responsible for determining the appropriate security marking for the information they produce or control, in any form (*e.g.*, paper, e-mails and other electronic documents, CDs and DVDs, etc).

When in doubt about the appropriate security marking, consult management or other knowledgeable personnel in your work area.

2. Security Marking Basics

2.1 The GC Security Marking Systems

- All Government of Canada (GC) employees are responsible for safeguarding information and assets under their control. Security markings are one of the means used to safeguard information and ensure its proper handling.
- The GC security marking systems for protected and classified information are based on the *Access to Information Act* and the *Privacy Act*, collectively known as ATIP. Unless some or all of the information in question qualifies for exemption[1] under one or both of these acts, you must mark it as "UNCLASSIFIED" (see Annex 1).
- If some or all of the information **does** qualify for exemption, you **must** label it with the appropriate security marking from either the protection system or the classification system, according to the criteria in sections 4 and 5.
- A document may contain various pieces of information that, taken individually, would require different security markings. When this is the case, determine the **highest** level of security marking required and apply it to the entire document.
- The author / originator of a document is responsible for exercising judgement in determining its security marking, ensuring that an accurate marking appears on each page of the document, and that the marking conforms to CSE style norms (section 2.2).

Continued on next page

[1] Refer to sections 13-26 of the *Access to Information Act*, and sections 18-28 of the *Privacy Act*.

2. Security Marking Basics, continued

2.2 CSE Style Norms for Security Markings

- CSE style norms for applying security markings conform to those established by the Treasury Board Secretariat. These require that security markings appear on the **top right corner** of each page, with the protection or classification level and any subsequent Control System Markings (*e.g.*, SI) in block capitals. Any Dissemination Control Markings (*e.g.*, Canadian Eyes Only) that follow this may or may not be in block capitals.
- In addition to the placement of the security marking on the top right corner (below the CSE badge, where applicable), the following information should be contained in the header or footer of a document:
  - the document's name and date
  - the pagination formula "Page X of Y"
  - the name of the issuing entity (title page only), and
  - the CERRID number of the document (title page only).

3. Government of Canada Security Markings

3.1 PROTECTED Information

- Protected information, if compromised, could conceivably harm an individual or other private interests (those of a company, for example).
- This information is considered to be in the **non-national interest**, meaning its compromise would not harm Canada as a whole.
- This kind of information must be marked as "PROTECTED A", "PROTECTED B" or "PROTECTED C", depending on the likely degree of injury its unauthorized disclosure would cause (see 4.1).

3.2 CLASSIFIED Information

- Classified information, if compromised, could conceivably harm Canada as a whole, such as its economy, its political stability, its relations with other countries, or its military or intelligence-gathering capabilities, to cite a few examples.
- This information is deemed to be in the **national interest** and must be marked as "CONFIDENTIAL", "SECRET" or "TOP SECRET", depending on the likely degree of injury its unauthorized disclosure would cause (see 5.1).

4. Protecting Information in the Non-National Interest

4.1 The PROTECTED System: Basics

- Most protected information at CSE is personal or proprietary information, or decision-making advice to management.
- Sensitive information or information received in confidence from other governments or organizations must also be marked with the appropriate level of protection.
- To decide which level of protection to accord your information, use:
  1. The table below
  2. Section 7 – Selecting a Security Marking

Security Marking	Definition, Consequences of Compromise and Examples
PROTECTED C	**Exceptionally grave injury to the non-national interest** • Examples of consequences: catastrophic financial losses to an organization, serious harm to a person or loss of life • Examples of information: the identity of a police informant, the whereabouts of someone in a witness protection program, specifications of proprietary technology, etc.
PROTECTED B	**Serious injury to the non-national interest** • Examples of consequences: invasion of privacy, loss of reputation and/or competitive advantage, or negative impact on management decision-making • Examples of information: medical or financial or criminal histories of individuals, financial records of private companies, decision-support papers, audits, evaluations, performance reviews, etc.
PROTECTED A	**Injury to the non-national interest** • Examples of consequences: embarrassment, inconvenience, impediments to management decision-making, etc. • Examples of information: an individual's Social Insurance Number, Personal Record Identifier, completed security clearance form, unlisted phone numbers, certain types of advice to or by CSE management, etc.
UNCLASSIFIED	**No injury to the non-national interest**

5. Classifying Information in the National Interest

5.1 The CLASSIFIED System: Basics

- Since much of the classified information at CSE is derived from Communications Intelligence, the specific features of the SIGINT security marking system and the wider Five-Eyes context must be taken into account when marking such information. SIGINT uses the Control System Marking "SI" (Special Intelligence) as well as various other Sub-Control System and Dissemination Control markings.
- Classified information received from other governments must be accorded an equivalent classification level within the GC or the CSE SIGINT security marking systems. Alternatively, the foreign document may retain its original classification from the originating country if that is the established practice in a given case.
- To arrive at the most appropriate classification for your information, use:
    1. The table below
    2. Section 6 – Classifying SIGINT Information
    3. Section 7 – Selecting a Security Marking

Security Marking	Definition, Consequences of Compromise and Examples
TOP SECRET	**Exceptionally grave injury to the national interest** • Examples of consequences: threat to the stability of Canada or friendly nations, loss of life, exceptionally grave damage to relations with friendly governments, exceptionally grave damage to the effectiveness of extremely valuable intelligence operations, severe long-term damage to the Canadian economy • Examples of information: very sensitive operations, details of CSE's relationship with other intelligence organizations, etc.

Continued on next page

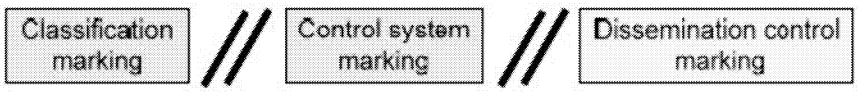
5. Classifying Information in the National Interest, continued

Security Marking	Definition, Consequences of Compromise and Examples
SECRET	**Serious injury to the national interest** • Examples of consequences: increased international tension, serious damage to international or federal-provincial relations, serious damage to valuable intelligence operations, significant threats to the national critical infrastructure or civil order, etc. • Examples of information: sensitive operations, Memoranda to Cabinet, operational plans of the Canadian Forces
CONFIDENTIAL	**Injury to the national interest** • Examples of consequence: damage to Canada's diplomatic relations, damage to the operational effectiveness of the Canadian forces, damage in the short term to economic interests, damage to the effectiveness of intelligence operations • Examples of information: general CSE capabilities (such as linguistic ability); lists of SIGINT clients at other departments
UNCLASSIFIED	**No injury to the national interest** • Examples of information: publicly available statements such as CSE's mandate according to the *National Defence Act*, or the fact that CSE collaborates with NSA, GCHQ, DSD, and GCSB (without details)

6. Classifying SIGINT Information

6.1 The SIGINT Security Marking System: Basics

- SIGINT documents typically have more complex security markings than non-SIGINT documents—Control System and Dissemination Control Markings usually demand more stringent handling requirements than for non-SIGINT documents.
- CSE SIGINT security markings are based on the GC classification system and common standards among CSE's SIGINT partners abroad.
- The SIGINT security marking system consists of three primary components:
  1. Classification,
  2. Control System Markings (and sometimes Sub-Control System Markings), and
  3. Dissemination Control Markings.
- **Compartmented Information** is any classified information to which access is controlled on a need-to-know basis through a formal control system (*e.g.*, SI or TK) or control sub-system (*e.g.*, GAMMA or ECI). A formal briefing and signed acknowledgement (indoctrination) is required before access to compartmented information is permitted.
- The components of a SIGINT security marking are separated by a double slash ("//"). A typical line might appear as follows:



e.g., TOP SECRET//SI//Canadian Eyes Only

- For more information on SIGINT classification lines, see *CSSS-103 SIGINT Classification Standards*.

7. Selecting a Security Marking

7.1 Introduction

Prior to marking information using the table in section 7.6 below, take the following points into consideration (7.2–7.5):

7.2 SIGINT documents

- When in doubt about how to classify SIGINT information, refer to *CSSS-103 SIGINT Classification Standards*, or to other CSE resources provided in the References section 8.2.

7.3 Security marking email, attachments, and calendar entries

- To mark emails *without* attachments, follow the steps in section 7.6.
- To mark emails *with* attachments, follow this rule:

  The email must bear the **highest** overall security marking of the email content and all attachments. **Never use a security marking on an email that is lower than that of the attachments.**
- An email saved in CERRID constitutes one record, whether it holds one email or a chain of emails. As such, the email marking and the CERRID profile marking must reflect the highest level of sensitivity contained within the email(s).
- The original sender in an email chain is considered to be the originator of the overall document and establishes the minimum protection or classification with his/her choice of security marking. The security marking applied to subsequent emails in the chain must not be lower than the originator's marking, but may be higher if new information in the chain warrants it.
- If someone in the email chain believes that the originator or another responder has applied a security marking incorrectly, he/she must not simply change the original marking; rather, the originator or other responder must be consulted and asked to resend the email using the proper marking.
- Emails referring to the URLs of classified websites on the secure internal network ("red" system), or emails containing CERRID references, do **not** need to be protected or classified **unless**:
  - the content of the email itself or an attached document requires protection or classification, or
  - the URL or CERRID reference itself discloses CSE sources, targets or methods.

Continued on next page

7. Selecting a Security Marking, continued

7.3 Security marking email, attachments, and calendar entries (continued)

- Email signature blocks must be unclassified; they must not refer to identifiable sources, targets or intelligence-gathering methods.
- Outlook calendar entries that contain protected or classified information must have an appropriate security marking added along the top of the text section.

7.4 Portion marking

- "Portion marking" refers to the practice (common in SIGINT) of assigning a security marking to each individual paragraph or information block of a document.
- The overall security marking of the document itself is equal to, and never less than, the highest security marking assigned to any of the paragraphs or information blocks. It must include **all** control system and sub-control system markings, and the **most restrictive** dissemination control marking.
- Portion marking is used because it:
  1. leads to more accurate security marking,
  2. facilitates sanitization and downgrading of information; and
  3. facilitates ATIP reviews.

7.5 Limiting distribution of UNCLASSIFIED material

- Much of the UNCLASSIFIED information at CSE is not intended for public release. While this information does not meet the exemption criteria under ATIP for protection or classification, or cause injury to the national or non-national interest, it could nevertheless be detrimental to CSE activities if it were made public. When combined, separate pieces of unclassified information can potentially yield sensitive information about CSE.
- CSE uses the dissemination control marking "**CSE Official Use Only**" (COUO) for unclassified information of this kind. This allows information to be shared with other organizations when appropriate in the context of CSE business. It can also be removed from CSE premises without specific packaging or authorization.
- Originators are responsible for determining what unclassified information should be marked "CSE Official Use Only".
- Recipients of COUO material should be instructed to handle it with discretion.

Continued on next page

7. Selecting a Security Marking, continued

7.6 Marking steps

Here are the steps to follow when marking information:

Step	Action
ATIP Check	Unless the information qualifies for exemption under the *Access to Information Act* (sections 13-26) or the *Privacy Act* (sections 18-28), it should be marked as "UNCLASSIFIED". Check section 7.5 above to decide whether "CSE Official Use Only" applies.
Interest Check	Ask yourself whether the information, if compromised, could damage any non-national (*i.e.*, private) interest, the national interest, or no interest at all. If the latter, then mark the document "UNCLASSIFIED". If it could damage a non-national interest, mark it PROTECTED A, B, or C (in conjunction with the injury check below). If it could damage the national interest, mark it "CONFIDENTIAL", "SECRET", or "TOP SECRET" (in conjunction with the injury check).
Injury Check	Ask yourself what specific harm to private or national interests could result or would likely result if the information were compromised. Consult the examples in tables 4.1 and 5.1.
Comparison Check	Compare the security marking you have selected with the security marking given to similar information or related documents.
Experience Check	Ask someone else more experienced in determining the security markings for sensitive information.

7. 7 Sanitizing, downgrading, declassifying, and destroying information

- In accordance with CSSS-100 (Chapter 2: Special Intelligence Classification and Markings), SIGINT and SIGINT-related information are not automatically declassified or downgraded. **s.15(1) - DEF**
- Sanitization is the process of

Continued on next page

[2] For more information on end-product sanitization or action-on procedures, contact Corporate and Operational Policy (D2).

7. Selecting a Security Marking, continued

s.15(1) - DEF

7. 7 Sanitizing, downgrading, declassifying, and destroying information (continued)

- CSE is Canada's sole authority for downgrading and declassifying SIGINT information and assets; all related requests must be referred to and approved by CSE's Corporate and Operational Policy section (@cse-cst.gc.ca on the internal secure network).
- For all other information, the authority to downgrade the classification or to declassify it altogether lies with the author or originator. In this person's absence, the authority lies with the originating section or department.
- ECI and GAMMA information must be destroyed in accordance with CSSS-102 *ECI Handling Standards* and CSSS-104 *GAMMA Handling Standards*, respectively.
- All classified or protected material, as well as "UNCLASSIFIED// CSE Official Use Only" material must be disposed of using an approved shredder[3] or burn bag.

8. Additional Information

8.1 Accountability

This table outlines responsibilities with respect to these procedures:

Who	Responsibility
Security Committee	Approving these procedures
All CSE personnel and any other parties acting under CSE's authority	Reading, understanding and complying with these procedures

8.2 References

SEC-103 refers to the following:

- *The Access to Information Act*
- *The Privacy Act*
- *Treasury Board Secretariat (TBS) Policy on Government Security (PGS)*
- *TBS Directive on Departmental Security Management (DDSM)*

Continued on next page

[3] All shredders at CSEC must be SI-approved Type II, Level 6 shredders.

7. Selecting a Security Marking, continued

8.2 References (continued)

- *TBS Security Organization and Administration Standard*
- *TBS Operational Security Standard: Management of Information Technology Security (MITS)*
- *Canadian SIGINT Security Standards (CSSS-100)*
- *ECI Handling Standards (CSSS-102)*
- *SIGINT Classification Standards (CSSS-103)*
- *Handling Requirements for Sensitive Material*

s.15(1) - DEF

8.3 Enquiries

Advice and guidance on security marking is available from:

- Corporate Security via ARS ("Corporate Security Policy")
- Corporate and Operational Policy via (for advice and guidance on SIGINT handling procedures only)
- SIGINT Security Management Office via (for advice and guidance on SIGINT security and the CSSS-series of policies)

8.4 Annexes

SEC-103 has the following two annexes:

- Annex 1 – Selecting a Security Marking
- Annex 2 – Handling Requirements for Sensitive Material

SEC-103 Annex 1: Selecting a Security Marking

The originators are responsible for determining the appropriate security markings for the information they produce or control. This chart walks you through the necessary steps.

Things to think about as you decide:
1. **Sensitivity** - meet any ATIP exemptions?
2. **Injury** – harm to the national interest or not?
3. **Consequences** - degree of damage?
4. **Control System** - sensitive sources/techniques?
5. **Dissemination Control** - limit distribution?

Sensitivity?
Does the information qualify for exemption under the *Access to Information* and/or *Privacy Acts* (ATIP) (*i.e.*, is it sensitive enough to be protected or classified)?

No → Security marking: **UNCLASSIFIED** → Then

Yes

Injury?
If the information were compromised, what injury or damage could be expected?

To a non-national interest
(*i.e*, an individual or organization)

To the national interest
(*e.g.*, Canada's economy, political stability, international relations, military or intelligence-gathering capabilities)

Consequences?
What consequences could reasonably be expected?

Consequences?
What consequences could reasonably be expected?

Injury	Serious injury	Exceptionally grave injury
(*e.g.*, embarrassment, inconvenience; also: information received in confidence from a foreign government)	(*e.g.*, invasion of privacy, loss of reputation and/or competitive advantage, negative impact on management decision-making)	(*e.g.*, catastrophic financial losses to an organization, serious harm to a person, loss of life)
Security marking: **PROTECTED A**	Security marking: **PROTECTED B**	Security marking: **PROTECTED C**

Injury	Serious Injury	Exceptionally grave injury
○ to Canada's diplomatic relations ○ to the operational effectiveness of the Canadian Forces ○ to short-term economic interests ○ to the effectiveness of intelligence operations	○ to international or federal-provincial relations ○ to the operational effectiveness of the Canadian Forces ○ to valuable intelligence operations ○ to national critical infrastructure ○ to civil order	○ to effectiveness or security of Canadian & allied forces ○ to relations with friendly governments ○ to the effectiveness of extremely valuable intelligence operations, ○ to the Canadian economy; ○ to Canada's stability or that of friendly nations; or ○ loss of life
Security marking: **CONFIDENTIAL**	Security marking: **SECRET**	Security marking: **TOP SECRET**

Controlled?
Does the information have to be handled within a special control system (*i.e.*, SI, TK) because it could potentially expose or compromise sensitive sources?

No → Dissemination?

Yes → Add the necessary **Control System Markings** (Refer to CSSS-103) → Then

Dissemination?
Should the dissemination of the document be limited in some way (*e.g.*, CSE Official Use Only, Management Eyes Only; Canadian Eyes Only)?

Yes → Add the necessary **Dissemination Control Markings** (Refer to SEC-103 or CSSS-103)

Need Help? Check similar documents, consult more experienced colleagues, or ask your manager or Group Security Officer.
Still have questions? Contact **Corporate Security** re: SEC-103. Contact the SIGINT Security Management Office re: CSSS-103.

Effective date: 26 February 2014

SEC-103 Annex 2: Handling Requirements for Sensitive Material

Introduction

Purpose

This annex sets out the **minimum** handling requirements at CSE for unclassified, protected, classified and Special Intelligence (SI) material, regardless of its format (hard copy, digital, etc.) — **anything less is a security violation**. These requirements also apply to equipment or devices that may not contain sensitive information, but that are sensitive in and of themselves (*e.g.*, due to sensitive capabilities).

The annex is organized according to what is being done with the sensitive material:

- Hand-carrying
- Mail / courier
- Electronic transmission
- Storage
- Destruction

Need to know

Sensitive information must only be shared with individuals who have the appropriate clearances and indoctrinations, as well as a valid requirement to access sensitive information in the performance of their duties — *i.e.*, they have a valid "need to know".

Safeguarding sensitive information is the responsibility of everyone holding a security clearance.

Maintaining control

When transporting protected or classified material, you **must** keep it in your possession/control at all times. When feasible, transmit it electronically (*e.g.*, secure email) instead of transporting it by hand.

The loss or theft of protected or classified material **must** be reported immediately to your manager or Group Security Officer (GSO).

Continued on next page

Introduction, continued

Registering the removal of sensitive material

Before removing classified or Protected C material from CSE, you **must** log it by completing the online Asset Removal Receipt Form. You must bring a print copy of the Asset Removal Receipt with you and present it to the guards if you are stopped for a random inspection — not having the required documents constitutes a security violation.[1]

When you remove sensitive equipment from CSE

The log must include sufficient detail to allow for an accurate damage assessment if the equipment is lost or stolen.

Asset Removal Receipts,

For designated individuals whose roles

the *Movement of Sensitive Assets (SEC-302)* policy allows for

Continued on next page

[1] If what you're removing is a trackable asset, you also need your manager's approval (*i.e.*, in an email) to remove it from the building. For more information on trackable assets, refer to the New Authorization Process for Removal of Trackable Assets and the Asset Management Policy.

Introduction, continued

Approved for use at CSE

All equipment used for transporting, storing, or destroying protected or classified material must be approved for use at CSE — this applies to hard-sided secure briefcases, Rifkin soft-sided secure briefcases, vinyl courier bags with tamper-evident security seals, secure cabinets, containers, locks, and shredders/disintegrators.

Secure briefcases must be purchased, logged, and tagged by Locksmith Services (except vinyl courier bags with tamper-evident security seals, which may be purchased by any group). Note that keys, combinations and passwords must safeguarded in a manner appropriate for the level of information they protect.

Protecting unclassified information

Even unclassified information can give hostile entities insight into CSE operations or personnel if enough bits are collected and pieced together. To protect against this "mosaic effect", all unclassified information that is work-related should be handled with discretion (*e.g.*, use an approved shredder or burn bag to dispose of it).

If information is unclassified but its public release could be detrimental to CSE's activities, mark it "**CSE Official Use Only**" (COUO) to control its dissemination. COUO information may be shared with other departments, organizations and partner agencies in the context of official business.

CSE locations and beyond

- "**To/from adjacent buildings**" means between buildings that share a secure perimeter:
  - between the Sir Leonard Tilley (SLT) building and Annex E, and
  - between the Edward Drake Building (EDB) and Annex F.
- "**On the CH campus**" means travelling among these buildings at Confederation Heights:
  - SLT building / Annex E,
  - EDB / Annex F,
  - Insurance Building (IB), and
  - Second floor of Canada Post Place (CPP).
- "**Within the NCR**" (National Capital Region) means anywhere off the Confederation Heights campus but within the amalgamated cities of Ottawa and Gatineau, including Pod 1 and Blair Place.
- "**Outside the NCR**" means outside the amalgamated cities of Ottawa and Gatineau.

Additional information

Policy references and other resources can be found on page 11.

A working aid summarizing the handling requirements is also available (CERRID #9927984).

HAND-CARRYING

"Single-wrapped"	"Double-wrapped"	
One of the following: • sealed self-addressed envelope with no security markings, • vinyl courier pouch secured with a tamper-evident security tab, • locked soft-sided Rifkin secure briefcase, or • locked hard-sided secure briefcase.	**1. One of the following:** • vinyl courier pouch secured with a tamper-evident security tab, or • sealed self-addressed envelope with security markings (if using an envelope for **Special Intelligence**, put security markings on both sides, top and bottom, and put security tape or reinforced tape over the seal.)	**2. Locked inside one of the following:** • soft-sided Rifkin secure briefcase, or • hard-sided secure briefcase

UNCLASSIFIED / UNCLASSIFIED//COUO	
Everywhere:	• No special handling requirements
PROTECTED A / PROTECTED B	
Inside a CSE building:	• Unsealed envelope, folder, vinyl courier pouch or equivalent
To/from adjacent buildings:	• Unzipped vinyl courier pouch, briefcase, or equivalent
On the CH campus:	• Single-wrapped
Within the NCR:	• Single-wrapped • Asset Removal Receipt is **recommended** but not required
Outside the NCR:	• Single-wrapped • Asset Removal Receipt is **recommended** but not required
PROTECTED C / CONFIDENTIAL / SECRET / TOP SECRET	
Inside a CSE building:	• Unsealed envelope, folder, vinyl courier pouch or equivalent
To/from adjacent buildings:	• Zipped vinyl courier pouch, briefcase, or equivalent
On the CH campus:	• Double-wrapped
Within the NCR:	• Double-wrapped • Asset Removal Receipt is **required** (ref. SEC 302) • If leaving material at a non-CSE destination, **must** ensure recipient has an approved security container; **must** have the recipient sign a completed transmittal receipt (GC-44)
Outside the NCR:	• Double-wrapped and **must** use a hard-sided secure briefcase • Asset Removal Receipt is **required** (ref. SEC-302) • If leaving material at a non-CSE destination, **must** ensure recipient has an approved security container; **must** have the recipient sign a completed transmittal receipt (GC-44) • Courier Certificate is **required** if travel involves security screening or if crossing an international border

s.15(1) - DEF

HAND-CARRYING (continued)

SPECIAL INTELLIGENCE (SI)	
Inside a CSE building:	• Unsealed envelope, folder, vinyl courier pouch or equivalent
To/from adjacent buildings:	• Zipped vinyl courier pouch, briefcase, or equivalent
On the CH campus:	• Double-wrapped
Within the NCR:	• Double-wrapped • Asset Removal Receipt is **required** (ref. SEC-302) • If leaving SI material at a non-CSE destination, **must** verify that the other party has the necessary indoctrination(s) and a SIGINT Secure Area (SSA) that is accredited to receive and store SI; **must** have the recipient sign a completed transmittal receipt (GC-44)
Outside the NCR:	• Double-wrapped and **must** use a hard-sided secure briefcase • Asset Removal Receipt is **required** (ref. SEC-302) • If leaving SI material at a non-CSE destination, **must** verify that the other party has the necessary indoctrination(s) and a SIGINT Secure Area (SSA) that is accredited to receive and store SI; must have the recipient sign a completed transmittal receipt (GC-44) • Courier Certificate is **required** if travel involves security screening or if crossing an international border to or from a NATO country (consult the SSMO before hand-carrying SI to a non-NATO country)

MAIL / COURIER

NOTE:

- When warranted by need-to-know or by clearance/indoctrination requirements, mark the envelope *"To be opened by addressee only"*.
- Mail sent through the CSE Mailroom to Pod 1, the LTA, Blair Place, or the warehouse is considered *internal* mail (note: mail sent to Blair Place must **not** be Protected C, classified, or SI). Mail sent to off-site Client Relations Officers (CROs) or to CFIOG is considered *external* mail.
- All external mail must go through the CSE Mailroom. Mailroom staff will prepare the outer envelope when one is required and route the mail through the appropriate channel (*e.g.*, Canada Post, special courier, etc.).
- s.15(1) - DEF is for **official use only** and for material that is Protected C, Confidential, Secret, Top Secret, or Special Intelligence (SI).

UNCLASSIFIED / UNCLASSIFIED//COUO	
Internal mail:	• Interoffice mail envelope (*i.e.*, reusable, with string closure) with no security markings
External mail:	• Sealed envelope with no security markings
PROTECTED A	
Internal mail:	• Sealed envelope with security markings
External mail:	• Sealed envelope with no security markings
PROTECTED B	
Internal mail:	• Sealed envelope with security markings
External mail:	• Double envelope (the CSE mailroom prepares the outer envelope) • On the inner envelope, put the recipient's address, a return address, and relevant security markings • Enclose a completed a transmittal receipt (GC-44) and mark the file or serial number on the front of the envelope • Seal the envelope and send it to CSE mailroom with a duplicate address label (including recipient phone number) for the outer envelope
PROTECTED C / CONFIDENTIAL / SECRET / TOP SECRET	
Internal mail:	• Sealed envelope with security markings
External mail:	• **Must** verify that the other party has the necessary clearance and security container • Double envelope (the CSE mailroom prepares the outer envelope) • On the inner envelope, put the recipient's address and a return address; put security markings on both sides, top and bottom • Enclose a completed a transmittal receipt (GC-44) and mark the file or serial number on the front of the envelope • Seal the envelope, put security tape or reinforced tape over the seal, and send it to CSE mailroom with a duplicate address label (including recipient phone number) for the outer envelope

MAIL / COURIER (continued)

SPECIAL INTELLIGENCE (SI)	
Internal mail:	• Sealed envelope with security markings
External mail:	• **Must** verify that the other party has the necessary indoctrination(s) and a SIGINT Secure Area (SSA) that is accredited to receive and store SI • Double envelope (the CSE mailroom prepares the outer envelope) • On the inner envelope, put the recipient's address and a return address; put security markings on both sides, top and bottom • Enclose a completed transmittal receipt (GC-44) and mark the file or serial number on the front of the envelope • Seal the envelope, put security tape or reinforced tape over the seal, and send it to CSE mailroom with a duplicate address label (including recipient phone number) for the outer envelope

ELECTRONIC TRANSMISSION

UNCLASSIFIED / UNCLASSIFIED//COUO	
Voice:	• May use an external non-secure phone ("black")
Fax:	• May use a non-secure fax; apply relevant security markings
Email:	• May use the external SABRE network ("black") or BlackBerry • Apply relevant security markings
PROTECTED A	
Voice:	• May use an external non-secure phone ("black")
Fax:	• May use a non-secure fax but the receiving fax must be in an operations zone (*i.e.*, access is limited to personnel who work there and visitors are escorted) • Apply relevant security markings
Email:	• May use the external SABRE network ("black"), including BlackBerry • Apply relevant security markings
PROTECTED B	
Voice:	• May use an external non-secure phone ("black")
Fax:	• May use a non-secure fax but the receiving fax must be in an operations zone • Apply relevant security markings • Notify the recipient before sending
Email:	• May use the external SABRE network ("black"), including BlackBerry, to send **only** to other CSE email addresses • **Must** encrypt using CSE-approved PKI when sending to non-CSE addresses; cannot use BlackBerry with PKI • Apply relevant security markings • For more information on email encryption, or acquiring and using a PKI certificate, contact the **IT Service Desk** via ARS.

ELECTRONIC TRANSMISSION (continued)

s.15(1) - DEF

PROTECTED C / CONFIDENTIAL / SECRET / TOP SECRET	
Voice:	• Must use an internal secure phone ("green") or external Secure Communications Interoperability Protocol (SCIP) phone (*e.g.*, • Ensure other party has the necessary clearance and is using a secure phone • Must ensure that unclassified phone conversations nearby are completed first
Fax:	• Must use a fax attached to an external SCIP phone • Apply relevant security markings • Ensure the other party has the necessary clearance and is using a secure fax • Notify the recipient before sending
Email:	• Must use an accredited secure network approved for the document's security marking • Apply relevant security markings • Ensure the other party has the necessary clearance
SPECIAL INTELLIGENCE (SI)	
Voice:	• Must use an internal secure phone ("green") or external SCIP phone accredited for SI • Must verify that other party has the necessary indoctrination(s) and is using a secure phone located in a SIGINT Secure Area (SSA) • Must ensure that unclassified phone conversations in the SSA are completed first
Fax:	• Must use a fax attached to an external SCIP phone accredited for SI • Apply all relevant security markings, including the SI control-system marking • Must verify that the other party has the necessary indoctrination(s) and is using a secure fax located in a SIGINT Secure Area (SSA) • Notify the recipient before sending
Email:	• Must use a secure network accredited for SI and approved for the document's security marking • Apply all relevant security markings including the SI control-system marking • Must verify that the other party has the appropriate indoctrination(s)

STORAGE

UNCLASSIFIED / UNCLASSIFIED//COUO	• No special storage requirements
PROTECTED A / PROTECTED B	• Must lock in workstation cabinet/drawer (unless in an area where an exception has been made to permit open storage)
PROTECTED C / CONFIDENTIAL / SECRET / TOP SECRET	• Must lock in an approved security cabinet with an integrated combination lock (unless in an area where an exception has been made to permit open storage)
SPECIAL INTELLIGENCE (SI)	• Must lock in an approved security cabinet with an integrated combination lock in a SIGINT Secure Area (unless in an area where an exception has been made to permit open storage).

DESTRUCTION

UNCLASSIFIED / UNCLASSIFIED//COUO	• Must use a burn bag or approved shredder/disintegrator. • For information regarding the destruction of CDs, DVDs, and other removable media, see *SEC-406-1 Removable Media Protection Standard*.
PROTECTED A / PROTECTED B	
PROTECTED C / CONFIDENTIAL / SECRET / TOP SECRET	
SPECIAL INTELLIGENCE (SI)	

RESOURCE MATERIAL

Document security markings	• *SEC-103 Protecting and Classifying Information*
Transporting sensitive material,	• *SEC-302 Movement of Sensitive Assets* • *SEC-303 Random Inspection Program*
Courier certificates	• *SEC-204-1 Foreign Travel Security and Crisis Procedures*
Security-related questions	• Contact Corporate Security via ARS
Removable media (*e.g.*, CDs, DVDs, USBs, etc.)	• *SEC-406-1 Removable Media Protection Standard* • Contact the Information Systems Security Officer (ISSO)
Trackable assets and the authorization process for the removal of trackable assets	• *Asset Management Policy* • Contact the Assets Management Group (F-help) via ARS
COMSEC handling	• *ITSD-03 Directive for the Control of COMSEC Material in the Government of Canada*
SIGINT security and control	• *CSSS-100 Canadian SIGINT Security Standards*
SIGINT classification	• *CSSS-103 The SIGINT Classification System*
GAMMA handling	• *CSSS-104 GAMMA Handling Standards* is currently under review — contact the SIGINT Security Management Office (@cse-cst.gc.ca)
Exceptionally Controlled Information (ECI) handling	• *CSSS-102 ECI Handling Standards*
SIGINT Security and CSSS-series policies	• Contact the SIGINT Security Management Office @cse-cst.gc.ca)
Corporate and operational policies	• Contact Corporate and Operational Policy (D2) @cse-cst.gc.ca)
E-mail encryption	• Contact the IT Service Desk via ARS

s.15(1) - DEF

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Corporate Security Directorate

UNCLASSIFIED
CSE Official Use Only

Handling Requirements for Sensitive Material – Working Aid

This working aid summarizes the **minimum** handling requirements for sensitive material at CSE — for more detail, see *SEC-103 Protecting and Classifying Information* (and annexes) and *CSSS-100 Canadian SIGINT Security Standards*.
Sensitive information must **only** be shared with individuals who have the appropriate clearances and indoctrinations, as well as a valid "need to know".
If leaving material at a non-CSE destination, you **must** ensure the recipient has an approved security container that, in the case of Special Intelligence, is in an accredited SIGINT Secure Area (SSA). The loss, theft, or compromise of protected or classified information **must** be reported immediately to your manager or Group Security Officer.

MARKINGS	UNCLASSIFIED UNCLASSIFIED// COUO	PROTECTED A	PROTECTED B	CONFIDENTIAL SECRET / TOP SECRET PROTECTED C	SPECIAL INTELLIGENCE (SI)

HAND-CARRYING

EXPLANATIONS FOR WRAPPING / PACKAGING REQUIREMENTS

- **Single-wrapped** = sealed self-addressed envelope with no security markings
  OR vinyl courier pouch secured with a tamper-evident security tab
  OR locked soft-sided Rifkin secure briefcase
  OR locked hard-sided secure briefcase
- **Double-wrapped** = sealed self-addressed envelope with security markings
  OR vinyl courier pouch secured with a tamper-evident security tab
  locked inside a hard-sided secure briefcase OR soft-sided Rifkin secure briefcase
- **Double-wrapping SI**: If using an inner envelope, must put security markings on both sides, top and bottom, and put security tape or reinforced tape over the seal

No special handling requirements

Inside a CSE building
Unsealed envelope, folder, vinyl courier pouch, or equivalent

To/from adjacent buildings
Unzipped vinyl courier pouch, briefcase, or equivalent

On the CH campus
Single-wrapped

Within the NCR
- Single-wrapped
- Asset Removal Receipt **recommended** but not required

Outside the NCR
- Single-wrapped
- Asset Removal Receipt **recommended** but not required

To/from adjacent buildings
Zipped vinyl courier pouch, briefcase, or equivalent

On the CH campus
Double-wrapped (extra instructions for **SI**, see above)

Within the NCR
- Double-wrapped (extra instructions for **SI**, see above)
- Asset Removal Receipt **required** (see SEC-302)
- If leaving material at a non-CSE destination, **must** have the recipient sign a completed transmittal receipt (GC-44)

Outside NCR
- Double-wrapped (extra instructions for **SI**, see above); **must** use hard-sided secure briefcase
- Asset Removal Receipt **required** (see SEC-302)
- If leaving material at a non-CSE destination, **must** have the recipient sign a completed transmittal receipt (GC-44)
- Courier certificate **required** if travel involves security screening or crossing a border to/from a NATO country (if going to a non-NATO country, consult Physical Security; if carrying **SI** material to a non-NATO country, consult the SSMO)

CH = Confederation Heights (SLT, EDB, IB, CPP)
To/from adjacent buildings = SLT to/from Annex E; EDB to/from Annex F
NCR = National Capital Region (includes to/from Pod 1, Blair Place, warehouse)

MAIL / COURIER

Internal
- Interoffice mail envelope (reusable, with string closure) with no security markings

External
- Sealed envelope with no security markings

Internal
Sealed envelope with security markings

External
- Double envelope – CSEC Mailroom prepares outer envelope (provide a duplicate address label)
- Inner envelope must have the recipient's address, a return address, security markings on both sides, top and bottom; enclose a completed transmittal receipt (GC-44) and mark file number or serial number on the envelope
- For Protected C, classified, and SI, put security tape or reinforced tape over envelope seal; send to mailroom

ELECTRONIC

Voice
May use an external non-secure phone ("black")

Fax
- May use a non-secure fax

Email
- May use external SABRE network ("black") or BlackBerry
- Add all security markings

Contact the IT Service Desk re: CSE-approved PKI encryption

Fax
- May use a non-secure fax but confirm that the receiving fax is in an "operations zone" (see SEC-103 Annex 2)
- Add all security markings
- Notify the recipient before sending Protected B

Email
- May use external SABRE network ("black") or BlackBerry to send to other CSE addresses.
- **Must** use CSE-approved PKI encryption for non-CSE addresses (PKI is **not** compatible with BlackBerrys)
- Add all security markings

Voice
- Must use an internal secure phone ("green") or external secure phone (accredited for **SI** if necessary)

Fax
- Must use a fax attached to an external secure phone (accredited for **SI** when relevant); ensure recipient is also using a secure fax
- Add all security markings (including **SI** markings when relevant)
- Notify The recipient before sending the fax

Email
- Must use an accredited secure network approved for the security level of the content (accredited for **SI** when relevant)
- Add all security markings (including **SI** markings when relevant)

STORAGE

- No special requirements
- Must lock in a workstation cabinet or drawer unless in an area where "open storage" is permitted by exception
- Must lock in an approved security cabinet with an integrated combination lock (in an SSA if storing **SI**) unless in an area where "open storage" is permitted by exception

Must use a burn bag or approved shredder/disintegrator
For information on the destruction of CDs, DVDs, and other removable media consult *SEC-406-1 Removable Media Protection Standard*

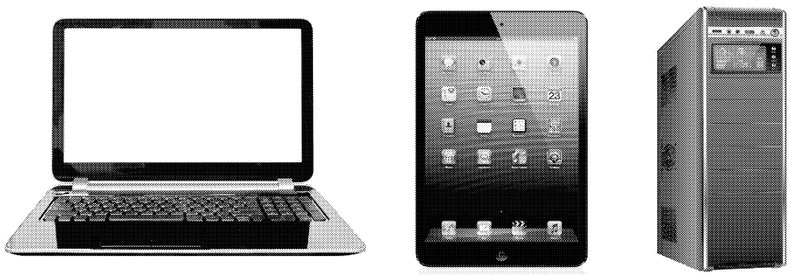
Communications Security Establishment | Centre de la sécurité des télécommunications

RESTRICTED ITEMS AT CSE

Do you have any recordable media or electronics with you?

If so, please leave them with the Commissionaire and pick them up as you leave.

COMPUTER/ LAPTOP/ TABLET

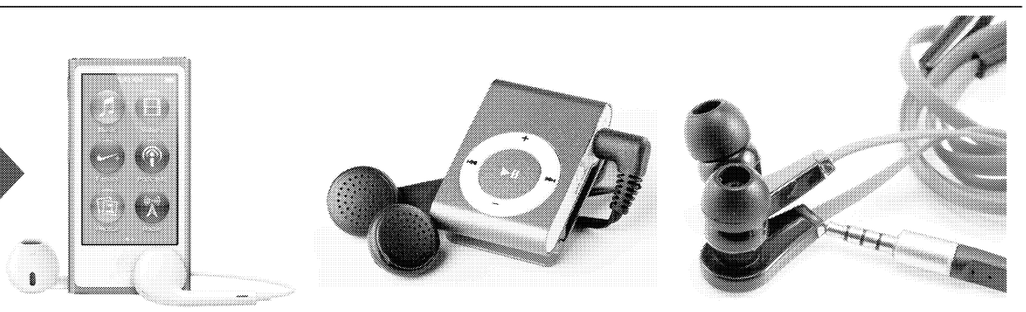


MOBILE DEVICES

- Smartphone
- iPhone
- BlackBerry
- Pager
- PDA
- Rocket Stick or ExpressCard

MUSIC DEVICES

- iPod
- MP3 Player
- Earbuds

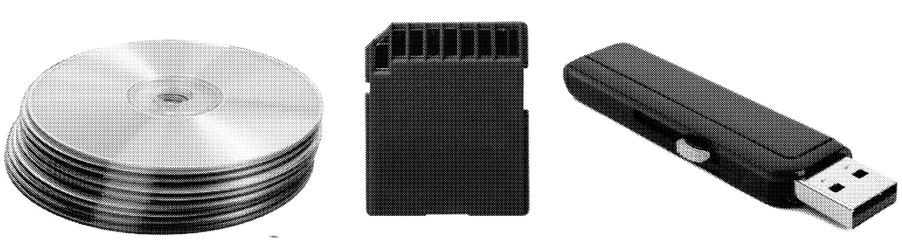


AUDIO/VISUAL EQUIPMENT

- Digital Camera
- Video Camera
- Audio Recorder

STORAGE DEVICES

- Writable/Rewritable CD and DVD
- Memory Card
- USB Stick
- External Hard Drive
- USB Cable



WEARABLE TECHNOLOGY

- Smartglasses
- Smartwatch
- Smartband
- Bluetooth Pendant
- USB Sunglasses
- USB Cufflinks
- Wearable Camera
- E-cigarette

Canada